

# Accounts: Introduction

- [Accounts Module Summary](#)
- [Understanding Access Levels](#)
- [Understanding User Status](#)
- [Understanding KAStrack's Password and Username Requirements](#)
- [Understanding My Channels](#)

# Accounts Module Summary

The Accounts Module is where all KAstrack user information (username, password, contact information, etc.) can viewed and managed. There are two pages in this module: My Accounts Page (each user has access) and the Accounts Page (for those given managerial access). Both pages are subdivided into tabs.

The Accounts Module has its own communication feature, called Channels, that serves as a commenting / bulletin board feature only visible to an individual and their supervisors. All accounts have one channel by default, called the Supervisor Channel. Additional channels can be created by administrators if desired.

# Understanding Access Levels

An Access Level is an authority designation in KAStack. There are four default Access Levels: Admin, Supervisor, Employee, and Observer. The permissions granted to each Access Level are outlined in the Site Settings Module on the Access Levels Tab. Customized Access Levels and the permissions associated with them can be created and customized for your organization. A user can have multiple Access Level designations but must be assigned one per module in order to access that module in KAStack.

By default, a user with an Admin Access Level will not be seen in the People Module unless they are also given the designation an Employee Access Level.

# Understanding User Status

The Status column designates if a KAStrack user is active or inactive. Inactive account parameters are established on the Inactive Accounts Tab in the Site Settings Module.

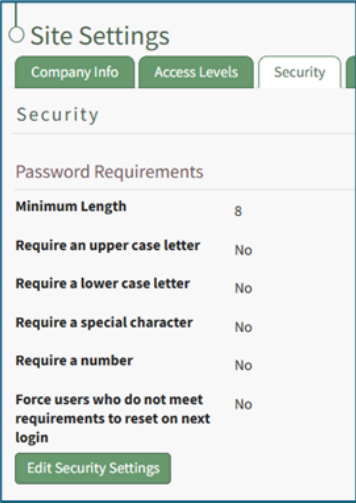
# Understanding KAStack's Password and Username Requirements

The default settings in KAStack require passwords to be a minimum of 8 characters. By default, a temporary password is entered for a new user, who is required to update their password at initial login. Individuals with an Admin access level can alter password requirements by going to the Security Tab of the Site Setting Module.

All passwords created through an import of information will be designated as temporary.

## How To: Edit Password Requirements

To edit password requirements, open the Security Tab in the Site Settings Module. The current settings will show before changes are made.



The screenshot shows the 'Site Settings' interface with the 'Security' tab selected. Under the 'Password Requirements' section, the following settings are displayed:

Requirement	Value
Minimum Length	8
Require an upper case letter	No
Require a lower case letter	No
Require a special character	No
Require a number	No
Force users who do not meet requirements to reset on next login	No

An 'Edit Security Settings' button is located at the bottom of the settings list.

Select the "Edit Security Settings" button, opening an editable Password Requirements Page.

The screenshot shows the 'Site Settings' interface with the 'Security' tab selected. Under 'Password Requirements', the 'Minimum Length' is set to 8. The checkboxes for 'Require an upper case letter', 'Require a lower case letter', 'Require a special character', 'Require a number', and 'Force users who do not meet requirements to reset on next login' are all currently unchecked. 'Save' and 'Cancel' buttons are at the bottom.

Input a whole number as your preferred minimum length requirement into the textbox.

Select the appropriate checkboxes to require users to have an uppercase letter, lowercase letter, special character, and/or number in the password.

Selecting the “Force users who do not meet requirements to reset on next login” checkbox will require any existing users whose password is no longer compliant to reset their password when they attempt to login next.

New users will be forced to meet the requirements when they login for the first time / register their account.

This screenshot is identical to the first one, but with the checkboxes for 'Require an upper case letter', 'Require a lower case letter', and 'Require a number' now checked. The 'Minimum Length' remains at 8, and the 'Force users...' checkbox remains unchecked.

Click “Cancel” to return to the Security Tab without making any changes.

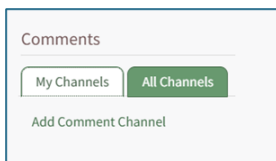
Select the “Save” button and return to the Security Tab. The changes made and saved are now reflected on the Security Tab.

Username can only include alphabetical lowercase letters, numbers, hyphens (-), underscores (\_), periods (.), or "at" signs (@). No other special characters or spaces are permitted, and usernames cannot start with an underscore.

# Understanding My Channels

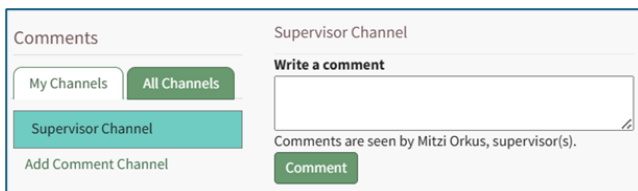
The Accounts Module has its own communication feature referred to as Channels that allows for comments to be sent between individuals and their supervisors and for comments to be shared between supervisory roles only. A date and time stamp are assigned to each comment as it is sent. An individual can access Channels on the Account Info Tab on the My Account Page.

For individuals with Supervisor and Admin module level access, channels are divided into two tabs: My Channels and All Channels.



The My Channels Tab will list all comment channels that an individual has access to.

The All Channels Tab will list all comment channels. The Supervisor Channel is a default channel that allows comments to be made that are accessible by an individual and that individual's supervisors.



Only individuals with Admin module access will see the clickable "Add Comment Channel" link.

If an individual does not have access to the channel the statement, "You do not have permission to view this channel because you are not a participant," will show in place of the comment textbox.

